CLAIMS

1. An apparatus for proving authentication when a user is not present, said apparatus comprising:

a Web service client coupled to a service provider;

a Web service provider; and

a discovery service;

wherein:

said Web service client, said service provider, said Web service provider, and said discovery service agree to work with each other; and

said Web service provider is configured in such a way such that said calling Web service client must prove that it has permission to request a service from said Web service provider when a live authenticated session of said user with said Web service client is not present.

2. The apparatus of Claim 1, wherein said Web service client comprises an assertion, said assertion comprising a statement that said user has an authenticated session.

3. The apparatus of Claim 2, wherein said assertion is signed by an authority.

4. The apparatus of Claim 3, wherein said authority is an identity provider of said discovery service.

5. The apparatus of Claim 2, wherein said statement comprises, but is not limited to, the following information:

a system entity that made said assertion;

a system entity making a request;

a system entity relying on said assertion; and

a name identifier of said user in a namespace of said system entity that made said assertion to said system entity relying on said assertion.

6. The apparatus of Claim 5, wherein said system entity making said assertion is an identity provider of said discovery service.

7. The apparatus of Claim 5, wherein said system entity making a request is said Web service client.

8. The apparatus of Claim 5, wherein said system entity relying on said assertion is said Web service provider.

9. The apparatus of Claim 5, wherein said asserting party is said Web service client and said relying party is said Web service provider.

10. The apparatus of Claim 2, wherein said statement is included in an extended assertion that is given to said service provider at time of authentication.

11. The apparatus of Claim 1, further comprising:

means for said Web service client presenting to said discovery service a service assertion obtained from a second system entity, wherein said service assertion comprises a user presence statement; and

means for said discovery service issuing a new service assertion comprising a new user presence statement, said new service assertion and said new user presence statement associated with said second system entity.

12. The apparatus of Claim 11, wherein said second system entity is a second Web service client.

13. The apparatus of Claim 1, further comprising means for said discovery service recording and storing user statement information.

14. The apparatus of Claim 13, wherein said recorded and stored user statement information is in the form of a table.

15. The apparatus of Claim 1, further comprising means for said Web service provider storing a ticket for checking said permission to request a service.

16. The apparatus of Claim 1, further comprising means for testing a request to said Web service provider while a user is still present, wherein either or both said discovery service and said Web service provider can perform real-time consent informational data collection from a user without having actually performed a particular transaction.

17. A method for proving authentication when a user is not present, said method comprising the steps of:

providing a Web service client coupled to a service provider;

providing a Web service provider; and

providing a discovery service;

wherein:

said Web service client, said service provider, said Web service provider, and said discovery service agree to work with each other; and

said Web service provider is configured in such a way such that said calling Web service client must prove that it has permission to request a service from said Web service provider when a live authenticated session of said user with said Web service client is not present.

18. The method of Claim 17, wherein said Web service client comprises an assertion, said assertion comprising a statement that said user has an authenticated session.

19. The method of Claim 18, wherein said assertion is signed by an authority.

20. The method of Claim 19, wherein said authority is an identity provider of said discovery service.

21. The method of Claim 18, wherein said statement comprises, but is not limited to, the following information:

a system entity that made said assertion;

a system entity making a request;

a system entity relying on said assertion; and

a name identifier of said user in a namespace of said system entity that made said assertion to said system entity relying on said assertion.

22. The method of Claim 21, wherein said system entity making said assertion is an identity provider of said discovery service.

23. The method of Claim 21, wherein said system entity making a request is said Web service client.

24. The method of Claim 21, wherein said system entity relying on said assertion is said Web service provider.

25. The method of Claim 21, wherein said asserting party is said Web service client and said relying party is said Web service provider.

26. The method of Claim 18, wherein said statement is included in an extended assertion that is given to said service provider at time of authentication.

27. The method of Claim 17, further comprising the steps of:

said Web service client presenting to said discovery service a service assertion obtained from a second system entity, wherein said service assertion comprises a user presence statement; and

said discovery service issuing a new service assertion comprising a new user presence statement, said new service assertion and said new user presence statement associated with said second system entity.

28. The method of Claim 27, wherein said second system entity is a second Web service client.

29. The method of Claim 17, further comprising the step of said discovery service recording and storing user statement information.

30. The method of Claim 20, wherein said recorded and stored user statement information is in the form of a table.

31. The method of Claim 17, further comprising the step of said Web service provider storing a ticket for checking said permission to request a service.

32. The method of Claim 17, further comprising the step of testing a request to said Web service provider while a user is still present, wherein either or both said discovery service and said Web service provider can perform real-time consent informational data collection from a user without having actually performed a particular transaction.

33. A method for invoking authenticated transactions on behalf of a user when the user is not present, said method comprising the steps of:

a service provider, at a time when a user is present, asking the user if said service provider can perform a particular transaction at a later point in time when the user is not present, wherein if the user indicates yes, then said service provider sending a notification to register with any of, or both of:

a trusted discovery service; and

a Web service provider that performs said particular transaction;

wherein while the user is still present, the user can be asked to provide informational content related to said particular transaction; and

for invocation, said service provider making a request of the Web service provider to perform said particular transaction.

34. The method of Claim 33, further comprising the step of a discovery service checking if the user gave permission for contacting said Web service provider when the user is not present, and if permission is granted, allowing control to go to said Web service provider.

35. The method of Claim 33, further comprising any of the steps of said Web service provider:

trusting said discovery service performed checking for permission and accepting that if said discovery service indicates the user gave permission, then said Web service provider performing said particular transaction; and

said Web service provider deciding to perform checking for permission, and subsequently performing said particular transaction if said Web service provider determines permission is granted.

36. The method of Claim 33, further comprising the step of providing a user capability of reviewing and modifying stored permissions.

37. The method of Claim 33, further comprising the step of providing robust security by having trust kept centrally in said discovery service.

38. The method of Claim 33, further comprising said discovery service supporting a plurality of different types of Web service providers.

39. An apparatus for invoking authenticated transactions on behalf of a user when the user is not present, said method comprising:

providing a service provider, at a time when a user is present, asking the user if said service provider can perform a particular transaction at a later point in time when the user is not present, wherein if the user indicates yes, then said service provider sending a notification to register with any of, or both of:

a trusted discovery service; and

a Web service provider that performs said particular transaction;

wherein while the user is still present, the user can be asked to provide informational content related to said particular transaction; and

for invocation, means for said service provider making a request of the Web service provider to perform said particular transaction.

40. The apparatus of Claim 39, further comprising means for a discovery service checking if the user gave permission for contacting said Web service provider when the user is not present, and if permission is granted, allowing control to go to said Web service provider.

41. The apparatus of Claim 39, further comprising means for any of said Web service provider:

trusting said discovery service performed checking for permission and accepting that if said discovery service indicates the user gave permission, then said Web service provider performing said particular transaction; and said Web service provider deciding to perform checking for permission, and subsequently performing said particular transaction if said Web service provider determines permission is granted.

42. The apparatus of Claim 39, further comprising means for providing a user capability of reviewing and modifying stored permissions.

43. The apparatus of Claim 39, further comprising means for providing robust security by having trust kept centrally in said discovery service.

44. The apparatus of Claim 39, further comprising means for said discovery service supporting a plurality of different types of Web service providers.